

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2000-076135
 (43) Date of publication of application : 14.03.2000

(51) Int.CI.

G06F 12/14
 G06K 17/00
 G06K 19/073
 G06K 19/07

(21) Application number : 10-242304

(71) Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

(22) Date of filing : 27.08.1998

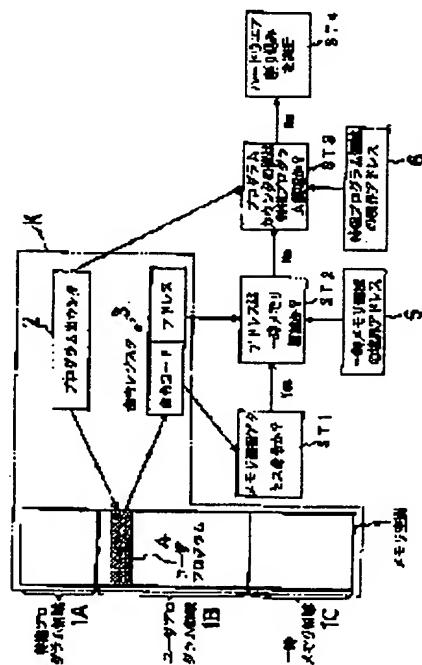
(72) Inventor : HOSODA YASUHIRO
 SUZUKI KATSUHIKO

(54) MEMORY PROTECTIVE METHOD FOR PROCESSOR AND IC CARD FOR PROTECTING MEMORY OF PROCESSOR

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the memory protective method of a processor and an IC card for protecting the memory of the processor capable of inhibiting unauthorized access to the memory and securing security even when a program is added to the memory.

SOLUTION: Together with the memory for dividing a memory space 1 into a privilege program area 1A for storing a variety of common service programs, a user program area 1B for storing a user program 4 downloaded by terminal equipment and a temporary memory area 1C to be temporarily used at the execution of the respective programs stored in the user program area 1B and the privilege program area 1A, a control means for performing access from the user program 4 to somewhere other than the temporary memory area 1C through a monitor and stopping the execution of the user program 4 for the unauthorized access to somewhere other than the temporary memory area 1C is provided.



LEGAL STATUS

[Date of request for examination] 18.04.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-76135

(P2000-76135A)

(43)公開日 平成12年3月14日 (2000.3.14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 06 F 12/14	3 2 0	G 06 F 12/14	3 2 0 A 5 B 0 1 7
G 06 K 17/00		G 06 K 17/00	E 5 B 0 3 5
19/073		19/00	P 5 B 0 5 8
19/07			N

審査請求 未請求 請求項の数24 O.L (全 9 頁)

(21)出願番号	特願平10-242304	(71)出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22)出願日	平成10年8月27日 (1998.8.27)	(72)発明者	細田 泰弘 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(72)発明者	鈴木 勝彦 東京都新宿区西新宿三丁目19番2号 日本 電信電話株式会社内
		(74)代理人	100071113 弁理士 菅 隆彦

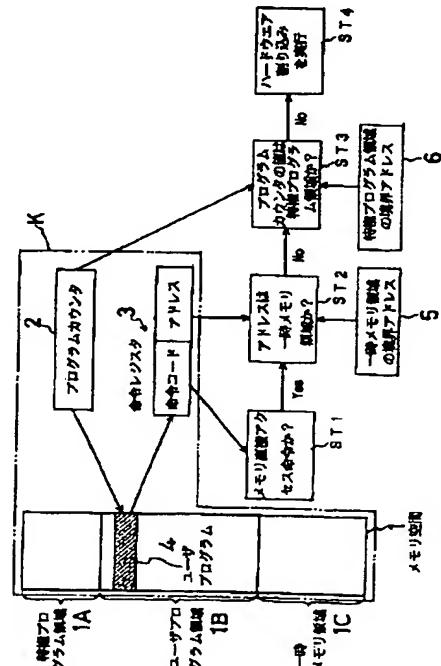
最終頁に続く

(54)【発明の名称】 プロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカード

(57)【要約】

【課題】メモリへの不正アクセスを禁止し、メモリにプログラムが追加されてもセキュリティ確保を可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカードの提供。

【解決手段】メモリ空間1を、種々の共通サービスプログラムを格納する特権プログラム領域1Aと、端末装置によりダウンロードされたユーザプログラム4を格納するユーザプログラム領域1Bと、ユーザプログラム領域1-B及び特権プログラム領域1Aに格納された各プログラムの実行時に一時的に使用する一時メモリ領域1Cとに区分するメモリと共に、ユーザプログラム4から一時メモリ領域1C以外へのアクセスはモニタを経由して行い一時メモリ領域1C以外への不正なアクセスはユーザプログラム4の実行を止める制御手段を具備するという特徴。



【特許請求の範囲】

【請求項1】C P Uとメモリとを有するプロセッサに小規模のハードウエアの追加とロジックにより、当該プロセッサのメモリ領域にユーザプログラムを追加・変更しても、当該メモリ領域への不正なアクセスを不可能にする、

ことを特徴とするプロセッサのメモリ保護方法。

【請求項2】小規模のハードウエアは、
ウインドウ回路を含む、

ことを特徴とする請求項1に記載のプロセッサのメモリ保護方法。

【請求項3】追加・変更は、
前記プロセッサ対応の端末装置により行われる、
ことを特徴とする請求項1又は2に記載のプロセッサのメモリ保護方法。

【請求項4】プロセッサは、
I Cカード用である、
ことを特徴とする請求項1、2又は3に記載のプロセッサのメモリ保護方法。

【請求項5】プロセッサは、
C P Uとメモリを有する1チップマイクロコンピュータ用である、
ことを特徴とする請求項1、2又は3に記載のプロセッサのメモリ保護方法。

【請求項6】メモリは、
各種共通のサービスプログラムを格納する特権プログラム領域と、
前記変更・追加されたユーザプログラムを含むユーザプログラムを格納するユーザプログラム領域と、
前記特権プログラム領域、前記ユーザプログラム領域に格納されたプログラムが実行される際に一時的に使用される一時メモリ領域との三領域に区分される、
ことを特徴とする請求項1、2、3、4又は5に記載のプロセッサのメモリ保護方法。

【請求項7】一時メモリ領域は、
前記メモリに格納された如何なるプログラムを実行するに当たり何の制約も受けない、
ことを特徴とする請求項6に記載のプロセッサのメモリ保護方法。

【請求項8】ロジックは、
プログラムカウンタの値が前記ユーザプログラム領域を指している場合には、
前記一時メモリ領域へのアクセスのみを許可すると共に他の領域へのアクセスでは例外処理を行う様に制御される、
ことを特徴とする請求項6又は7に記載のプロセッサのメモリ保護方法。

【請求項9】例外処理は、
ハードウエアの割り込みを生じさせることにより開始される、

ことを特徴とする請求項8に記載のプロセッサのメモリ保護方法。

【請求項10】ロジックは、
前記ユーザプログラム領域に格納されたユーザプログラムから前記一時メモリ領域以外へアクセスの必要性がある場合には、
前記アクセスの正当性の確認を行う、
ことを特徴とする請求項6、7、8又は9に記載のプロセッサのメモリ保護方法。

【請求項11】アクセスの正当性の確認は、
前記特権プログラム領域に格納されたサービスプログラムを呼出した後に、
前記サービスプログラムにより前記アクセスの正当性の判断を行う、
ことを特徴とする請求項10に記載のプロセッサのメモリ保護方法。

【請求項12】判断は、
前記呼出しの前に前記ユーザプログラムが必要とする、
前記ユーザプログラム領域のデータに対応した保護キーに相当する情報と当該データのアドレスを前記一時メモリ領域に書き込み、
前記呼出しの後、
前記サービスプログラムにより、前記一時メモリ領域に書き込まれた前記保護キーに相当する情報と、前記ユーザプログラム領域に格納された前記データの保護キーとを照合した結果、一致すれば、アクセスの許可をする、
ことを特徴とする請求項11に記載のプロセッサのメモリ保護方法。

【請求項13】アクセスの許可は、
前記データを前記一時メモリ領域に複写した後に、
制御を前記ユーザプログラムに戻す、
ことを特徴とする請求項12に記載のプロセッサのメモリ保護方法。

【請求項14】メモリ領域を、
種々の共通サービスプログラムを格納する特権プログラム領域と、
端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、
当該ユーザプログラム領域及び前記特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、
前記ユーザプログラムから前記一時メモリ領域以外へのアクセスはモニタを経由して行い、当該一時メモリ領域以外への不正なアクセスに対して当該ユーザプログラムの実行を止める制御手段を具備する、
ことを特徴とするプロセッサのメモリを保護されたI Cカード。

【請求項15】制御手段は、
プログラムカウンタの値が前記ユーザプログラム領域を指している際は前記一時メモリ領域以外の直接アクセス

を禁止し、当該一時メモリ領域以外へのアクセスが必要な際は当該特権プログラム領域に存在するサービスプログラムを経由し、当該特権プログラム領域を指している際は全てのメモリ領域へのアクセスを可能とする制御手段である、

ことを特徴とする請求項14に記載のプロセッサのメモリを保護されたICカード。

【請求項16】制御手段は、

前記プログラムカウンタの値を読み出した後に指定された番地の命令を読み出す命令フェッチ回路と、

当該命令フェッチ回路から前記指定された番地の命令を格納する命令レジスタと、

当該命令レジスタの値をデコードする命令デコード回路と、

当該命令デコード回路に接続されたアドレス演算回路と、

前記命令デコード回路に接続されたラッチと、

前記プログラムカウンタに接続され前記特権プログラム領域の境界アドレスとの関係を判断するウインドウ回路と、

前記アドレス演算回路の出力結果及び演算終了通知を受け、一時メモリ領域の境界アドレスとの関係を判断する別のウインドウ回路と、

前記ラッチと前記ウインドウ回路と前記別のウインドウ回路との各出力を判断する論理回路と、

当該論理回路からの出力により、前記プログラムカウンタに予め特権プログラム領域に設けてある割り込みベクトルによりアドレスをロードする割り込み回路と、を具備する、

ことを特徴とする請求項14又は15に記載のプロセッサのメモリを保護されたICカード。

【請求項17】命令デコード回路は、

当該命令デコード回路の前記命令レジスタの値に対する結果の実行が直接前記メモリ領域にアクセスを必要とする場合には、前記ラッチに対する出力をアサートすると共に前記アドレス演算回路を作動させる、

ことを特徴とする請求項16に記載のプロセッサのメモリを保護されたICカード。

【請求項18】制御手段は、

前記メモリと共に一体構成される、

ことを特徴とする請求項14、15、16又は17に記載のプロセッサのメモリを保護されたICカード。

【請求項19】共通サービスプログラムは、

前記ICカード上のファイルを管理するプログラムを含む、

ことを特徴とする請求項14、15、16、17又は18に記載のプロセッサのメモリを保護されたICカード。

【請求項20】ICカード上のファイルを管理するプログラムは、

データアクセス用サービスプログラムである、ことを特徴とする請求項19に記載のプロセッサのメモリを保護されたICカード。

【請求項21】前記データアクセス用サービスプログラムは、

前記ユーザプログラム領域に格納されたユーザプログラムが前記一時メモリ領域以外にアクセス要求すると呼び出され、

前記ユーザプログラムが前記一時メモリ領域に書き込みした前記アクセス要求の正当性を示す保護キーに相当する情報及び前記アクセス要求先のアドレスを元にして、書き込まれた当該保護キーに相当する情報と前記ユーザプログラム領域に格納されたアクセス要求先のアドレスの情報に対応した保護キーとを照合した後、一致すれば前記アクセスを許可し実行する一連の処理プログラムである、

ことを特徴とする請求項20に記載のプロセッサのメモリを保護されたICカード。

【請求項22】一連の処理プログラムは、

前記アクセス要求先のアドレスの情報を、前記一時メモリ領域に複写し、

ユーザプログラムに戻る前記実行機能を含む、

ことを特徴とする請求項21に記載のプロセッサのメモリを保護されたICカード。

【請求項23】前記ウインドウ回路は、

前記特権プログラム領域の境界アドレスを固定化する特権プログラム領域の境界アドレス固定値回路に接続する、

ことを特徴とする請求項17、18、19、20又は21に記載のプロセッサのメモリを保護されたICカード。

【請求項24】前記別のウインドウ回路は、前記一時メモリ領域の境界アドレスを固定化する一時メモリ領域の境界アドレス固定値回路に接続する、ことを特徴とする請求項17、18、19、20、21又は22に記載のプロセッサのメモリを保護されたICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード等のセキュリティを必要とする分野に使用される1チップマイクロコンピュータ上のユーザプログラムからの不正メモリアクセスに対して保護する、プロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカードである。

【0002】

【従来の技術】従来、ICカード用の1チップマイクロコンピュータ(チップ)は、マスクロム上にプログラムを、EEPROM等の不揮発性メモリにユーザデータを格納し、外部端末装置より発行されるコマンドをマスク

ロム上に書き込まれたプログラムが解釈し実行するものが一般的であった。そして、マスクロム上に書き込まれたプログラムは外部からソフト的な手段により破壊することは不可能であるため、予めマスクロム作成者により十分なセキュリティ上の確認を経て作成されたプログラムはユーザデータに対する権限外の不当なアクセスは起きないと考えられている。

【0003】しかしながら、最近のICカードアプリケーションの拡大に伴い、一度発行したICカード上にプログラムの追加・変更を、ICカードアプリケーション発行機関から要求されているのが現状である。これは、ユーザにとっても複数のカードを持ち歩く必要性がなく、一枚のICカードで複数のサービスを享受できる点で利点が大きい。

【0004】この要求を実現するために、ユーザデータだけでなくアプリケーションプログラムも不揮発性メモリに記憶させ、チップ作成後にダウンロードにより変更・追加が可能とするICカードが登場している。

【0005】

【発明が解決しようとする課題】上記のようなICカードでは、チップ作成時において既にICアプリケーションが他のアプリケーションが有するデータへの不正なアクセスを不可能とすることを確認するのは無理であるので、別途新たにメモリ保護機能を当該チップ内に持たす必要性がある。

【0006】このメモリ保護の実現方法として、先ずこれまでのプロセッサの歴史で確立されてきた種々のハード的な仕掛けをプロセッサ上に盛り込むことが考えられ、限界レジスタ方式、キー方式、アクセスコントロール方式、リングプロテクション方式（中澤喜三朗著「計算機アーキテクチャ構成方式」pp. 140-143、朝倉書店1995年）などが考えられる。

【0007】しかしながら、これらの方は元々マルチプログラミングを前提としており、現状のチップはシングルタスクであり、またICカード用チップは低コストが要求されるため、設計が複雑になること、ハード量の不必要的増加を招くこと、命令の実行時間が長くなることなどの面において問題をはらんでいる。

【0008】一方、ソフトのみでメモリ保護を実現することも選択肢としてありうる。これはいわゆる仮想計算機のチップ上に実装し、そこにメモリ保護機能を持たず方式である。Java Card (http://java.sun.com)、Multos (http://www.multos.com) 等はこの方式によっている。

【0009】しかしながら、この方式が意味を持つためには、チップ上へのCPUネイティブコードのダウンロードを禁止し、仮想計算機のコードのみを可とする必要がある。仮想計算機上では、メモリアクセスの正当性をソフトウェアにより確認するため性能上のオーバーヘッ

ドがあり、10倍乃至数十倍程度の実行性能が低下することを回避することができない。

【0010】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。

【0011】本発明の第1の目的は、簡便なハードウェアによりメモリの不正アクセスを禁止し、プロセッサ上にプログラムを追加してもセキュリティ確保を可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカードを提供せんとするものである。

【0012】本発明の第2の目的は、複数のアプリケーションの性能をオーバーヘッドなく実行可能とするプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカードを提供せんとするものである。

【0013】本発明の第3の目的は、命令の実行に長時間を必要とせずにセキュリティを大幅に向上させるプロセッサのメモリ保護方法及びプロセッサのメモリを保護されたICカードを提供せんとするものである。

【0014】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0015】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、CPUとメモリとを有するプロセッサに小規模のハードウェアの追加とロジックにより、プロセッサのメモリ領域にユーザプログラムを追加変更しても、当該メモリ領域への不正なアクセスを不可能にするという特徴を有する。

【0016】本発明カードは、上記課題の解決に当たり、メモリ領域を種々の共通サービスプログラムを格納する特権プログラム領域と、端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、当該ユーザプログラム領域及び当該特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、当該ユーザプログラムから当該一時メモリ領域以外へのアクセスはモニタを経由して行い当該一時メモリ領域以外への不正なアクセスは当該ユーザプログラムの実行を止める制御手段を具備するという特徴を有する。

【0017】更に、具体的に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、上記目的を達成するように為される。

【0018】本発明方法の第1の特徴は、CPUとメモリとを有するプロセッサに小規模のハードウェアの追加とロジックにより、当該プロセッサのメモリ領域にユーザプログラムを追加変更しても、当該メモリ領域への不正なアクセスを不可能にするプロセッサのメモリ保護方法の構成採用にある。

【0019】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における小規模のハードウェアが、ウイ

ンドウ回路を含んでなるプロセッサのメモリ保護方法の構成採用にある。

【0020】本発明方法の第3の特徴は、上記本発明方法の第1又は第2の特徴における追加・変更が、前記プロセッサ対応の端末装置により行われてなるプロセッサのメモリ保護方法の構成採用にある。

【0021】本発明方法の第4の特徴は、上記本発明方法の第1、第2又は第3の特徴におけるプロセッサが、I Cカード用であるプロセッサのメモリ保護方法の構成採用にある。

【0022】本発明方法の第5の特徴は、上記本発明方法の第1、第2又は第3の特徴におけるプロセッサが、CPUとメモリを有する1チップマイクロコンピュータ用であるプロセッサのメモリ保護方法の構成採用にある。

【0023】本発明方法の第6の特徴は、上記本発明方法の第1、第2、第3、第4又は第5の特徴におけるメモリが、各種共通のサービスプログラムを格納する特権プログラム領域と、前記変更・追加されたユーザプログラムを含むユーザプログラムを格納するユーザプログラム領域と、前記特権プログラム領域、前記ユーザプログラム領域に格納されたプログラムが実行される際に一時的に使用される一時メモリ領域との三領域に区分されてなるプロセッサのメモリ保護方法の構成採用にある。

【0024】本発明方法の第7の特徴は、上記本発明方法の第6の特徴における一時メモリ領域が、前記メモリに格納された如何なるプログラムを実行するに当たり何の制約も受けないプロセッサのメモリ保護方法の構成採用にある。

【0025】本発明方法の第8の特徴は、上記本発明方法の第6又は第7の特徴におけるロジックが、プログラムカウンタの値が前記ユーザプログラム領域を指している場合には、前記一時メモリ領域へのアクセスのみを許可すると共に他の領域へのアクセスでは例外処理を行う様に制御されてなるプロセッサのメモリ保護方法の構成採用にある。

【0026】本発明方法の第9の特徴は、上記本発明方法の第8の特徴における例外処理が、ハードウェアの割り込みを生じさせることにより開始されてなるプロセッサのメモリ保護方法の構成採用にある。

【0027】本発明方法の第10の特徴は、上記本発明方法の第6、第7、第8又は第9の特徴におけるロジックが、前記ユーザプログラム領域に格納されたユーザプログラムから前記一時メモリ領域以外へのアクセスの必要性がある場合には、前記アクセスの正当性の確認を行つてなるプロセッサのメモリ保護方法の構成採用にある。

【0028】本発明方法の第11の特徴は、上記本発明方法の第10の特徴におけるアクセスの正当性の確認が、前記特権プログラム領域に格納されたサービスプログラムを呼出した後に、前記サービスプログラムにより

前記アクセスの正当性の判断を行つてなるプロセッサのメモリ保護方法の構成採用にある。

【0029】本発明方法の第12の特徴は、上記本発明方法の第11の特徴における判断が、前記呼出し前に前記ユーザプログラムが必要とする、前記ユーザプログラム領域のデータに対応した保護キーに相当する情報と当該データのアドレスを前記一時メモリ領域に書き込み、前記呼出しの後、前記サービスプログラムにより、前記一時メモリ領域に書き込まれた前記保護キーに相当する情報と、前記ユーザプログラム領域に格納された前記データの保護キーとを照合した結果、一致すれば、アクセスの許可を行なつてなるプロセッサのメモリ保護方法の構成採用にある。

【0030】本発明方法の第13の特徴は、上記本発明方法の第12の特徴におけるアクセスの許可が、前記データを前記一時メモリ領域に複写した後に、制御を前記ユーザプログラムに戻してなるプロセッサのメモリ保護方法の構成採用にある。

【0031】一方、本発明カードの第1の特徴は、メモリ領域を、種々の共通サービスプログラムを格納する特権プログラム領域と、端末装置によりダウンロードされたユーザプログラムを格納するユーザプログラム領域と、当該ユーザプログラム領域及び前記特権プログラム領域に格納された各プログラムの実行時に一時的に使用する一時メモリ領域とに区分するメモリと共に、前記ユーザプログラムから前記一時メモリ領域以外へのアクセスはモニタを経由して行い、当該一時メモリ領域以外への不正なアクセスに対して当該ユーザプログラムの実行を止める制御手段を具備してなるプロセッサのメモリを保護されたI Cカードの構成採用にある。

【0032】本発明カードの第2の特徴は、上記本発明カードの第1の特徴における制御手段が、プログラムカウンタの値が前記ユーザプログラム領域を指している際は前記一時メモリ領域以外の直接アクセスを禁止し、当該一時メモリ領域以外へのアクセスが必要な際は当該特権プログラム領域に存在するサービスプログラムを経由し、当該特権プログラム領域を指している際は全てのメモリ領域へのアクセスを可能とする制御手段であるプロセッサのメモリを保護されたI Cカードの構成採用にある。

【0033】本発明カードの第3の特徴は、上記本発明カードの第1又は第2の特徴における制御手段が、前記プログラムカウンタの値を読み出した後に指定された番地の命令を読み出す命令フェッチ回路と、当該命令フェッチ回路から前記指定された番地の命令を格納する命令レジスタと、当該命令レジスタの値をデコードする命令デコード回路と、当該命令デコード回路に接続されたアドレス演算回路と、前記命令デコード回路に接続されたラッチと、前記プログラムカウンタに接続され前記特権プログラム領域の境界アドレスとの関係を判断するウイ

ンドウ回路と、前記アドレス演算回路の出力結果及び演算終了通知を受け、一時メモリ領域の境界アドレスとの関係を判断する別のウインドウ回路と、前記ラッチと前記ウインドウ回路と前記別のウインドウ回路との各出力を判断する論理回路と、当該論理回路からの出力により、前記プログラムカウンタに予め特権プログラム領域に設けてある割り込みベクトルによりアドレスをロードする割り込み回路と、を具備してなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0034】本発明カードの第4の特徴は、上記本発明カードの第3の特徴における命令デコード回路が、当該命令デコード回路の前記命令レジスタの値に対する結果の実行が直接前記メモリ領域にアクセスを必要とする場合には、前記ラッチに対する出力をアサートすると共に前記アドレス演算回路を作動させてなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0035】本発明カードの第5の特徴は、上記本発明カードの第1、第2、第3又は第4の特徴における制御手段が、前記メモリと共に一体構成されてなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0036】本発明カードの第6の特徴は、上記本発明カードの第1、第2、第3、第4又は第5の特徴における共通サービスプログラムが、前記ICカード上のファイルを管理するプログラムを含んでなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0037】本発明カードの第7の特徴は、上記本発明カードの第6の特徴におけるICカード上のファイルを管理するプログラムが、データアクセス用サービスプログラムであるプロセッサのメモリを保護されたICカードの構成採用にある。

【0038】本発明カードの第8の特徴は、上記本発明カードの第7の特徴におけるデータアクセス用サービスプログラムが、前記ユーザプログラム領域に格納されたユーザプログラムが前記一時メモリ領域以外にアクセス要求すると呼び出され、前記ユーザプログラムが前記一時メモリ領域に書き込みした前記アクセス要求の正当性を示す保護キーに相当する情報及び前記アクセス要求先のアドレスを元にして、書き込まれた当該保護キーに相当する情報と前記ユーザプログラム領域に格納されたアクセス要求先のアドレスの情報に対応した保護キーとを照合した後、一致すれば前記アクセスを許可し実行する一連の処理プログラムであるプロセッサのメモリを保護されたICカードの構成採用にある。

【0039】本発明カードの第9の特徴は、上記本発明カードの第8の特徴における一連の処理プログラムが、前記アクセス要求先のアドレスの情報を、前記一時メモリ領域に複写し、ユーザプログラムに戻る前記実行機能を含んでなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0040】本発明カードの第10の特徴は、上記本発

明カードの第4、第5、第6、第7又は第8の特徴における前記ウインドウ回路が、前記特権プログラム領域の境界アドレスを固定値化する特権プログラム領域の境界アドレス固定値回路に接続してなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0041】本発明カードの第11の特徴は、上記本発明カードの第4、第5、第6、第7、第8又は第9の特徴における前記別のウインドウ回路が、前記一時メモリ領域の境界アドレスを固定値化する一時メモリ領域の境界アドレス固定値回路に接続してなるプロセッサのメモリを保護されたICカードの構成採用にある。

【0042】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を示すカード例及び方法例を説明し、更にカード例、方法例を用いた実施例をあげて説明する。

【0043】(カード例)図1は、本カード例のプロセッサのメモリを保護されたICカードKに関する基本構成を示したものであり、同時に(下記する)カード例に対応する方法例の流れについても示したものである。なお、同図は説明上重要な部分のみを示しており、プログラムカウンタ2、命令レジスタ3の他通常のプロセッサ(特にマイクロプロセッサ)に具備されるレジスタ、出入力関連、クロック等は図示していないが、一般の論理回路、デジタル回路、情報回路等にして周知であるので省略する。

【0044】本カード例の対象は、1チップ上に通常の計算機でいう外部記憶、内部記憶が集積されるため、特に区別することなく、一つのメモリ空間1上の領域として考えることが可能である。そこで、この一つのメモリ空間1を三区分し、メモリ空間1を特権プログラム領域1A、ユーザプログラム領域1B、一時メモリ領域1Cとする。

【0045】特権プログラム領域1Aは、ICカードK上のファイル管理をはじめとする各種の共通のサービスプログラムを格納される領域である。ユーザプログラム領域1Bは、(図示しない)端末装置からダウンロードされたユーザプログラム4が格納される領域である。一時メモリ領域1Cは、特権プログラム領域1Aに格納された特権プログラム、ユーザプログラム4が実行時に一時的に使用する領域である。

【0046】ここで、特権プログラムからは全てのメモリ空間1への読み書き可能である。しかし、ユーザプログラム4からは一時メモリ領域1Cのみがアクセス可能であり、それ以外の領域への不正なアクセスを試みるとハードウェア割込みを生ぜしめユーザプログラム4の実行を中断する。

【0047】(方法例)本方法例は、上記カード例に適用させたものであり、図1を参照しながら説明する。

【0048】ICカードKのメモリ空間1上に格納され

るプログラムはプログラムカウンタ2の値に従って読み出され、逐次デコード、実行される。この命令デコードの際、メモリの内容をアクセスする要求が命令中に含まれている否かを判断する(ST1)。

【0049】もし含まれている場合には、(1)プログラムカウンタ2の値が、特権プログラム領域1Aを指していれば、全ての領域へのアクセスを許可し、(2)プログラムカウンタ2の値がユーザプログラム領域1Bを指していれば、一時メモリ領域1Cへのアクセスのみ許可する。他の領域へのアクセスであれば、ハードウェア割り込みを生じさせ、例外処理を開始する(ST2、ST3、ST4)。ここで、ユーザプログラム4から一時メモリ領域1C以外へのアクセスが必要であれば、特権プログラム領域1Aに格納されているサービスプログラムを呼び出し、サービスプログラムはアクセス要求が正当なものかを判断した上で許可するか否かを決定する。

【0050】なお、本方法例は、ICカードKのみならず、通常のCPUとメモリを有する1チップマイクロコンピュータであっても良い。

【0051】

【実施例】(実施例1) 図2は、上記本実施形態例の実施例を示したものである。同図を参照しながら、説明する。

【0052】(1) 命令フェッチ回路7は、プログラムカウンタ2の値を読み出し、そこで指定されている番地の命令をメモリ8よりメモリ入出力回路9を介して読み出し、命令レジスタ3に格納する。

【0053】(2) 命令レジスタ3の値は、命令デコード回路10によりデコードされ、その結果に従い命令が実行される。ここで、当該命令が直接メモリ8領域へのアクセスを必要とするものであれば、信号線11がアサートされると同時にアドレス演算回路12が動作しアドレス演算を開始する。信号線11の情報はラッチ13に取り込まれる。ここで、ラッチ13は、内部状態を持つ回路で、クロックの立ち上げ又は立ち下げにより入力信号を取り込み、内部状態がそのまま出力信号になる回路である。

【0054】(3) アドレス演算が終了し演算終了通知14がアサートされた時点で、ウインドウ回路15はアドレス演算回路12からのアドレス出力16のアドレスと一時メモリ領域1Cの境界アドレス固定値回路5'による一時メモリ領域1Cの境界アドレス5との関係を判断し、一時メモリ領域1Cを外れているときは出力線をアサートする。

【0055】(4) ウインドウ回路17は、プログラムカウンタ2の値と特権プログラム領域1Aの境界アドレス固定値回路6'による特権プログラム領域1Aの境界アドレス6との関係を判断し、プログラムカウンタ2の値が特権プログラム領域1Aを外れているときは出力線をアサートする。ここで、ウインドウ回路15、17

は、プログラムカウンタ2の値PCと境界アドレス(AD1、AD2、但しAD1<AD2)を比較し、IF PC<AD1 OR PC>AD2 THEN 1(アドレスは境界領域を外れているので1を出力する) ELS E 0 という動作をする回路である。

【0056】(5) 2つのウインドウ回路15、17からのそれぞれの出力及びラッチ13からの出力の論理和を論理和回路18によりとり、全てがアサートされたとき、割り込み要求出力をアサートする。

【0057】(6) 割り込み要求がアサートされると、(図示しない) 割り込み要求回路はプログラムカウンタ2に予め特権プログラム領域1Aの設けてある割り込みベクトルによりアドレスをロードし、割り込み処理を開始する。

【0058】以上の実施例1では、実質的にウインドウ回路15、17を付け加え簡単なロジックにより実現することができるが、本発明の目的を達し下記する効果を奏する他の回路構成、ロジックをとっても何等問題はない。

【0059】(実施例2) 図3は、上記実施例1とは別の実施例を示したものである。同図を参照しながら、本実施例を説明する。

【0060】(1) ユーザプログラム領域1Bは、複数のユーザプログラム(ユーザプログラムA α 、ユーザプログラムB β 、 \dots)と複数のデータ(データA γ 、データB δ 、 \dots)を有し、当該データにはそれぞれ保護キー(保護キーA ϵ 、保護キーB ζ 、 \dots)が付けられている。

【0061】(2) もし、ユーザプログラムA α がデータA γ を読み出す必要が生じたときは、ユーザプログラムA α はデータA γ のアドレスと保護キーに相当する情報を一時メモリ領域1Cに書き込み(ST5)、特権プログラム領域1Aにあるデータアクセス用サービスプログラム η を呼び出す(ST6)。

【0062】(3) サービスプログラム η は、一時メモリ領域1C上に書き込まれた保護キーとデータAの保護キー ϵ を照合し、一致すればアクセスを許可する。このときデータA γ の情報は一時メモリ領域1Cに複写され、制御はユーザプログラムA α に戻る。

【0063】これにより、データの持つ保護キーを予め知っているユーザプログラム以外のアクセスは禁止でき、セキュリティを確保することができる。

【0064】以上、本発明のカード例、方法例を説明し、更に、その実施例について説明したが、本発明は、プロセッサのメモリを保護すると共に、同時に、メモリのアクセス制御方式について示したものであり、本発明の見方により、プロセッサのメモリ保護方法はプロセッサのメモリアクセス方法としても見ることができ、また、プロセッサのメモリが保護されたICカードは、プロセッサのメモリアクセスが制御されたICカードとし

て見ることもできる。

【0065】

【発明の効果】以上説明したように、本発明によれば、小規模なハードウエア（実質的にはウインドウ回路2つ）の追加と簡単なロジックによりチップのセキュリティを大幅に向上させることができるので、ICカード上へのネイティブコードのダウンロードが可能となり、複数のアプリケーションを性能のオーバーヘッドなく実行することができ、多種多様の要請に応えることができる等の優れた効果を奏する。

【図面の簡単な説明】

【図1】本発明の実施の形態の基本構成を示したものである。

【図2】本発明の実施例1を示したものである。

【図3】本発明の実施例2を示したものである。

【符号の説明】

K … ICカード

1 … メモリ空間

1A … 特権プログラム領域

1B … ユーザプログラム領域

1C … 一時メモリ領域

2 … プログラムカウンタ

3 … 命令レジスタ

4 … ユーザプログラム

5 … 一時メモリ領域の境界アドレス

5' … 一時メモリ領域の境界アドレス固定値回路

6 … 特権プログラム領域の境界アドレス

6' … 特権プログラム領域の境界アドレス固定値回路

7 … 命令フェッチ回路

8 … メモリ

9 … メモリ入出力回路

10 … 命令デコード回路

11 … 信号線

12 … アドレス演算回路

13 … ラッチ

14 … 演算終了通知

15, 17 … ウインドウ回路

16 … アドレス出力

18 … 論理和回路

α … ユーザプログラムA

β … ユーザプログラムB

γ … データA

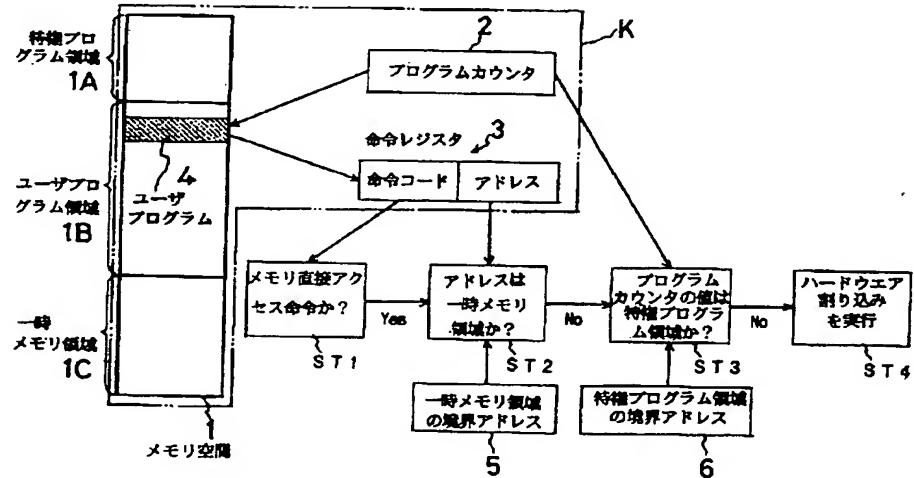
δ … 保護キーA

ε … データB

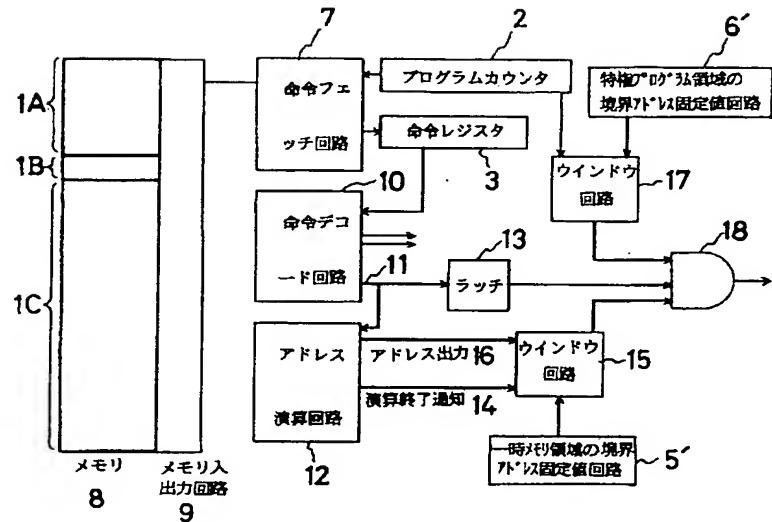
ζ … 保護キーB

η … データアクセス用サービスプログラム

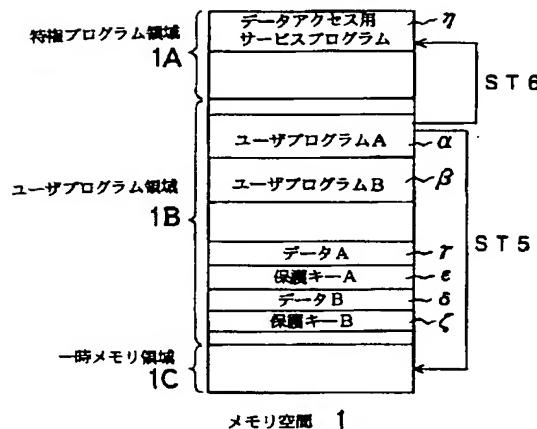
【図1】



【図2】



【図3】



フロントページの続き

Fターム(参考) 5B017 AA01 BA01 BA02 BB01 BB03
 CA13 CA14 CA15
 5B035 AA13 BB09
 5B058 CA28 KA31